SecureWay® Boundary Server for Windows NT® and AIX

概説

バージョン 2.0

GC88-8558-00
(英文原典：GC31-8733-00)

SecureWay® Boundary Server for Windows NT® and AIX

概説

バージョン 2.0

GC88-8558-00
(英文原典：GC31-8733-00)

お願い

本書、および本書で記述する製品をご使用になる前に、 41ページの『付録B. 特記事項』 を必ずお読みください。

本書は、IBM SecureWay Boundary Server 製品のバージョン 2、リリース 0、モディフィケーション・レベル 0 に適用されます。また、改訂版などで特に断りのない限り、これ以降のすべてのリリースにも適用されます。

本マニュアルについてご意見やご感想がありましたら

http://www.ibm.com/jp/manuals/main/mail.html

からお送りください。今後の参考にさせていただきます。
なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.infocr.co.jp/ifc/books/

をご覧ください。（URL は、変更になる場合があります）

原　典： GC31–8733–00
IBM SecureWay® Boundary Server for Windows NT® and AIX
Up and Running
Version 2.0

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 1999.11

目次

本書について

本書は、Windows NT® 版および AIX 版の IBM SecureWay®Boundary Server のインストール、構成、使用、およびトラブルシューティングを計画する方法について説明します。

SecureWay Boundary Server のインストールと構成を行う前に、ファイアウォール、VPN (仮想私設網)、コンテンツ・セキュリティー、およびネットワーク管理について正確な知識を持っていることが重要です。ネットワークに出入りするアクセスを制御するファイアウォールのセットアップと構成を行うことになるので、まず最初に、ネットワークの操作方法を理解する必要があります。特に、IP アドレス、完全修飾名、およびサブネット・マスクについての基本を理解している必要があります。

本書の対象読者

本書は、IBM SecureWay Boundary Sever のインストール、管理、および使用を行う、ネットワークまたはシステムのセキュリティー管理者を対象としています。

西暦 2000 年対応

これらの製品は、2000 年対応になっています。本製品と一緒に使用されるすべての製品 (たとえば、ハードウェア、ソフトウェア、およびファームウェア) が、正確な日付データを本製品と正しく交換する場合、本製品は、関連資料にしたがって使用すれば、20 世紀と 21 世紀内の日付データ、および 20 世紀と 21 世紀間の日付データを正しく処理し、提供し、受信することができます。

サービスおよびサポート

IBM SecureWay FirstSecure オファリングに含まれているすべての製品に対するサービスとサポートについては、IBM にお問い合わせください。これらの製品の中には、IBM 以外のサポートを参照しているものがあります。これらの製品を、FirstSecure オファリングの一部として取得する場合、サービスとサポートについて IBM にお問い合わせください。

本書の構成

本書には、以下の章が含まれています。

- 1ページの『第1章 SecureWay Boundary Server の概要』では、SecureWay Boundary Server とその構成要素の概要を説明します。
- 5ページの『第2章 IBM の SecureWay Boundary Server の紹介』では、SecureWay Boundary Server が必要な理由を示します。

- 19ページの『第5章 SecureWay Boundary Server のインストールおよび構成』では、Windows NT およびAIX オペレーティング・システムでの SecureWay Boundary Server のインストールと構成について説明します。
- 11ページの『第3章 SecureWay Boundary Server をインストールする前に』では、SecureWay Boundary Server の計画の方法について説明します。
- 17ページの『第4章 IBM SecureWay Boundary Server (SBS) の要件』には、SecureWay Boundary Server の最小必要条件を示します。
- 33ページの『第6章 関連資料』では、他の SecureWay Boundary Server の資料、および関連製品の資料の参照先を説明します。

表記規則

本書では、以下の表記規則を使用します。

表記規則	意味
太字	チェック・ボックス、ボタン、およびコマンドなどのユーザー・インターフェース要素。
モノスペース	SecureWay Boundary Server に関係する構文およびディレクトリーのデフォルト。
->	メニューからの一連の選択項目を表示します。たとえば、「**File -> Run**」は、「**File**」をクリックしてから、「**Run**」をクリックするという意味です。

Web 情報

SecureWay Boundary Server の最新の更新についての情報は、以下の Web アドレスで入手できます。

http://www.ibm.com/software/security/boundary/library

その他の IBM SecureWay FirstSecure 製品の更新についての情報は、以下の Web アドレスで入手できます。

http://www.ibm.com/software/security/firstsecure/library

新機能

SecureWay Boundary Server のバージョン 2.0 には、多くの新しい機能が含まれています。もっとも重要な新機能を、以下に挙げます。

SecureWay Policy Director との統合

SecureWay Policy Director は、ファイアウォールが SecureWay Boundary Server を使用可能にしていれば、ファイアウォール・プロキシー・ユーザーを管理することができます。ファイアウォール・プロキシー・ユーザーは、以下のファイアウォール・サービスで定義されます。

- Telnet
- FTP
- HTTP
- Socks

ユーザーとそれに関連するポリシーは、Lightweight Directory Access Protocol (LDAP) データベースに保管されます。

SecureWay Directory は、LDAP を提供して、保管、更新、検索、および交換用として中央設置場所にディレクトリー情報を保持します。 SecureWay Policy Director は、LDAP データベース内のファイアウォール・プロキシー・ユーザーを管理します。

経路指定の効率化

経路指定の効率化のために、Finjan SurfinGate プラグインを使用して、コンテンツのフィルター処理のための回線のネットワーク・トラフィックを少なくしています。

割り込みのブロッキング

コマンド・ラインのプログラムによって、ファイアウォール上に動的「拒否」規則を作成します。割り込みのブロッキングを、自動化スクリプトの中に組み込むことができます。

IBM SecureWay Firewall 4.1

IBM SecureWay Firewall for Windows NT は、以下のものを提供します。

Remote Access Service

Windows NT Remote Access Service (RAS) は、2 地点間プロトコル (PPP) を使用して、ダイヤル呼び出し、ISDN、または X.25 媒体を介したネットワーク接続を提供します。 NDISWAN はネットワーキング・ドライバーの 1 つであり、RAS の一部として提供され、下部の PPP データを類似のイーサネット LAN データに変換します。

IBM SecureWay Firewall for AIX 4.1 の機能強化

IBM SecureWay Firewall for AIX は、以下のものを提供します。

拡張 IPSec サポート

IBM SecureWay Firewall 4.1 には、拡張された IPSec サポートが含まれており、これには、新しいヘッダーをサポートするトリプル DES 暗号化が含まれています。これはまた、いくつかの IBM サーバーとルーターの相互操作性、ならびに新しいヘッダーをサポートする多くの IBM 以外の VPN 製品の相互操作性もサポートします。

対称マルチプロセッサー (SMP)

ファイアウォールのユーザーは、スケーリングとパフォーマンスの向上のために、RS/6000 のマルチプロセッサー・フィーチャーを活用することができます。

フィルターの機能強化

フィルターは、構成を行うことによってより良いパフォーマンスを提供するよう、機能強化されました。異なるタイプのフィルター規則をどこに配置するかを選択することによって、ファイアウォールのパフォーマンスを調整することができます。さらに、接続が使用された回数がログに記録されます。

セットアップ・ウィザード

IBM SecureWay Firewall の初期構成を援助するウィザードです。このセットアップ・ウィザードによって、新規のユーザーは、IBM Firewall のインストールの後で、すみやかにファイアウォールの基本構成を立ち上げて、実行することができます。

Network Security Auditor

Network Security Auditor (NSA) は、ネットワーク・サーバーおよびファイアウォールに、セキュリティー上の欠陥や構成エラーがないかどうかを検査します。これは機能強化されて、より高速で、より強力になっています。

ドイツ語の各国語サポート

ブラジル語、ポルトガル語、英語、フランス語、イタリア語、日本語、韓国語、中国語 (簡体字)、スペイン語、中国語 (繁体字) に加えて、ドイツ語の各国語サポートが提供されるようになりました。

Network Address Translation

Network Address Translation (NAT) は、多対 1 のアドレス・マッピングをサポートするよう拡張されました。これらのマッピングは、複数の内部の未登録または私用のアドレスから、ポート番号を使用した登録済みの正規のアドレスに対して行うもので、固有のマッピングを作成します。

AIX および Windows NT でサポートされる共通機能

Security Dynamics ACE/Server

Security Dynamics ACE/Server は、認証の 2 つの要素を提供します。このフィーチャーは機能強化されて、偶発的な破壊または悪意を持った侵入の可能性から、ネットワークとデータ・リソースを保護します。

Secure Mail Proxy の機能強化

IBM Firewall Secure Mail Proxy は、以下の新しい機能が含まれるよう機能強化されています。

- わかっている spam (迷惑メール) 発信元からのメッセージのブロック化 (除外リスト) を含む spam 防止アルゴリズム、メッセージの妥当性検査と応答性検査 (希望しないメッセージをブロックする方法として知られている)、メール・メッセージの宛先の数の構成可能限界、メッセージの最大サイズの構成可能限界
- 強力な認証メカニズムの統合を含む詐称防止サポート
- SNMP トラップ・サポートおよび MADMAN MIB のサポート
- ファイアウォールとドミノ間のメッセージを継ぎ目なく追跡するための機能を含むメッセージ追跡

Socks プロトコルのバージョン 5 の機能強化

Socks プロトコルのバージョン 5 は、ユーザー ID とパスワードの認証 (UNPW)、チャレンジ / 応答認証 (CRAM)、および認証プラグインを含むようアップグレードされました。

ログ記録は、ログ・メッセージのクラス分けと、ログ・レベルの指定について、ユーザーがさらに制御できるよう機能強化されています。

HTTP プロキシー

IBM SecureWay Firewall は、IBM Web Traffic Express (WTE) 製品に基づいた、完全装備の HTTP プロキシー設定を提供します。 HTTP プロキシーは、IBM Firewall を通したブラウザー要求を効率的に処理するものであり、Web のブラウズのための socks サーバーが不要になります。ユーザーは、内部ネットワークのセキュリティーを損なうことなく、インターネット上の便利な情報にアクセスすることができます。ただし、ブラウザーは、HTTP プロキシーを使用するよう構成されている必要があります。

SecureWay 用の MIMEsweeper 2.0

MIMEsweeper は、**MAILsweeper 4.1_2**、**WEBsweeper 3.2_5**、および **WEBsweeper 1.0_2** という、3 つの主要な構成要素を持っています。以下にその機能強化の一部を挙げます。

MAILsweeper

MAILsweeper 4.1_2 for SMTP は、Content Technologies flagship MIMEsweeper 製品を大幅にアップグレードしたものです。以下の新しいフィーチャーを提供します。

- 使用しやすい階層構造のポリシー・アーキテクチャーは、適切な組織レベル (個々のユーザーまでのレベル) でポリシーを適用する柔軟性を備えています。
- 業界標準のグラフィカル・ユーザー・インターフェース (GUI) は、ソフトウェア構成、ポリシーの作成、および管理を単純化します。

- 新しい Split Delivery フィーチャーは、バージョン 4 の階層構造のポリシー設定のための機能です。複数の宛先を持つメッセージの場合、ポリシーは、それぞれの宛先に適用されます。許可された宛先はそのメッセージを受け取れますが、許可されていない宛先は拒否されます。
- マルチスレッドのメッセージ処理は、スループットを向上させ、 1 つまたは複数のスレッドでエラーが発生した場合は、残りのスレッドを使用してメッセージ処理を続行できるようにすることにより、処理能力を強化しています。
- 他のベンダーのアンチウィルス製品とともに、MAILsweeper は、メッセージや添付物でのウィルスの検出と除去を提供します。
- NEAR、AND、NOT、および OR 式を使用した高度なテキスト分析は、メッセージの構文またはアーキテクチャーに基づいた、包括的で効果的なシナリオの作成にきわめて大きな柔軟性を提供します。
- 拡張監査ツールにより、データをどの ODBC 準拠のデータベースにも送ることができます。
- Real-Time Black List (RBL) サーバーのサポートは、ジャンク E メールを送信することがわかっているサイトのブラック・リストを作成します。 MAILsweeper は、このリストに載っているホストからの接続の受け入れを拒否することができます。
- コンテンツ・セキュリティーは、電子メールのトラフィックについての魅力的なレポート / グラフ / 表を提供することで、管理を容易にします。
- LDAP ディレクトリーとの統合。
- Delivery Service Notification (DSN) は、 SNMP と NT Alerter をサポートするようになりました。

WEBsweeper

- 追加のパフォーマンス上の機能強化により、データ処理速度が向上します。
- HTTP および FTP のトラフィックに対して、ウィルス・スキャナーと一緒に作動します。

WEBsweeper HTTPS

- WEBsweeper は、新しい HTTPS プロキシー・ソリューションを使用して、Web ベースの e-commerce アプリケーションに対する完全サポートを提供するようになりました。

SurfinGate 4.05

SurfinGate の機能強化には、以下のものがあります。

JavaScript コンテンツ検査

SurfinGate 4.05 は、問題になる可能性のある JavaScript 操作を探して、企業のセキュリティー・ポリシーに違反する JavaScript を停止します。 SurfinGate 4.05 により、管理者は、JavaScript、Java、および ActiveX に対して、

VisualBasic Script 用の smart フィルター処理と cookie を使用して、中央から、ポリシーを設定して強制することができます。

重要な任務を持つもののパフォーマンスの監視

SurfinGate 4.05 には、異常動作 (実行時エラーなど) および障害時の SurfinGate の再始動を検出する自動ツールが含まれています。これは基本的に、重要な任務を持つエリアに対するセキュリティー・フィーチャーです。

ポリシー管理の増強

SurfinGate は、未解決のアプレット・プロファイルを、自動ブロッキング用のデータベースの中に入れます。それにより、管理者は、アプレット / コントロールのリストを編集することができます。

FTP および SSL プロトコルのサポート

SurfinGate 4.05 は、モバイル・コードについて、ファイル転送プロトコル (FTP) チャネルを監視して、インターネットから勝手に入り込んでくるコードを見張り続けます。 FTP に対する監視に加えて、SurfinGate は、 モバイル・コードについて、HTTP トラフィックを監視し、HTTPS トラフィックを追加の装置に渡します。

ファイアウォール HTTP プロキシーとのプラグイン統合

SurfinGate は、プロキシー・チェーンの中の 1 つのプロキシーとして働くか、または Windows NT 用のファイアウォール上で Web Traffic Express のプラグインを介して働きます。

第1章 SecureWay Boundary Server の概要

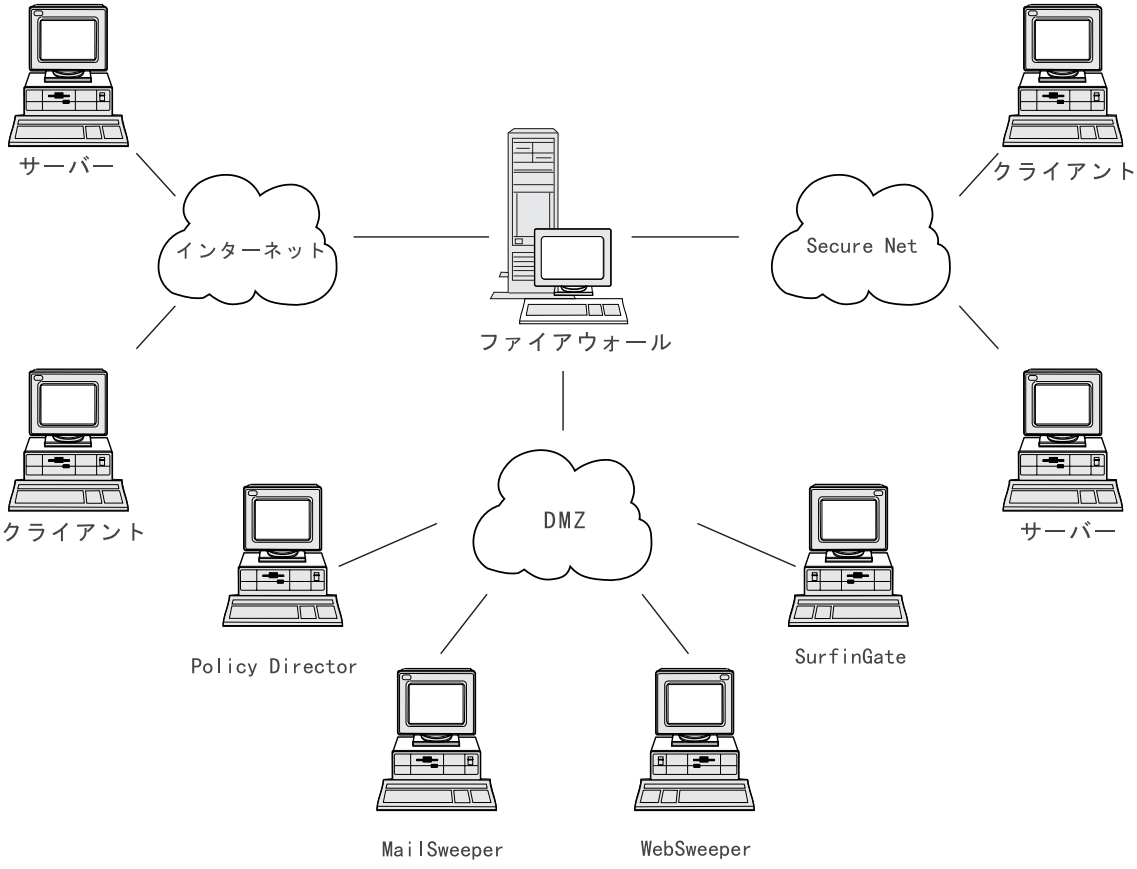


図 1. IBM SecureWay Boundary Server の構成例

この例は、MAILsweeper、WEBsweeper、Policy Director、および SurfinGate の各構成要素を使用する 5 つのワークステーションを図示したものであり、 Web トラフィックの監視と経路指定を行い、クライアントとサーバーの間でファイアウォールを使用してメールを転送します。この例では、5 つの物理的に分離されたワークステーションを使用します。

典型的な SecureWay Boundary Server の例

最小限のセットアップのためには、以下のマシンを使用することをお勧めします。

表 1. Boundary Server 構成要素製品のハードウェア要件

製品	マシン
IBM Firewall	Windows NT または AIX
MAILsweeper	Windows NT
WEBsweeper	Windows NT
SurfinGate	Windows NT

SecureWay Boundary Server をフルに利用したい場合は、 SecureWay Policy Director がネットワーク内に存在する必要があります。これによって、ファイアウォール・プロキシー・ユーザーは、 SecureWay Directory (LDAP) に保管することが可能になります。

HTTP の例 (Windows NT ファイアウォール): 典型的なシナリオでは、インターネット上のコンテンツに対する HTTP 要求は、クライアント・マシンから発信されます。この要求は、まず最初に WEBsweeper に流れます。アウトバウンド・パスでは、単純に、要求は WEBsweeper によって代行されて、ファイアウォール HTTP プロキシーに送られます。

ファイアウォール HTTP プロキシーでは、ユーザーが認証されます。これがセッションをブラウズしているクライアントからの最初の要求である場合は、ユーザー ID とパスワードの入力に挑戦できます。ユーザー ID は、Policy Director によって管理される LDAP データベースの中で、クライアントのセキュリティー・ポリシーを検索するのに使用されます。クライアントに対する HTTP 認証ポリシーによって、および入力されたパスワードの検査結果によって、その要求が拒否されるか、または先に進むことが許されます。認証操作のためには、さらに LDAP データベースか、または Security Dynamics ACE サーバーにアクセスすることが必要になる場合があります。同じブラウズのセッションからの後続の要求では、ブラウザーがユーザー ID とパスワードを自動的に提供することになります。クライアントはユーザー ID とパスワードの入力に挑戦できませんが、それぞれの要求は、最初の要求と同じプロセスで認証されることになります。

認証が成功すると、要求は、インターネット上の要求されたサーバーで代行して行われます。

インターネット・サーバーからコンテンツがファイアウォール HTTP プロキシーに戻されると、そのコンテンツは SurfinGate プラグインによって検査されます。ユーザーに対するグループ情報は、LDAP データベースから取得され、ポリシーの判断のためのベースにするために、プラグインで使用可能になります。コンテンツに SurfinGate に関係するものが入っていない場合、SurfinGate は、最小の処理オーバーヘッドで、プラグインを速やかにそのまま通過させます。 JavaScript に含まれているコンテンツは、プラグインでフィルター処理されます。コンテンツに Java または ActiveX が含まれている場合

は、フィルター処理のために SurfinGate サーバーに転送され、フィルター処理されたコンテンツがファイアウォール HTTP プロキシーに戻されます。 SurfinGate プラグインで処理された結果のコンテンツは、 WEBsweeper サーバーに送り返されます。

コンテンツが WEBsweeper サーバーに戻ってくると、サーバーは、WEBsweeper ポリシーにしたがってフィルター処理を行い、それをクライアントに戻します。

HTTP の例 (AIX ファイアウォール): AIX では、トラフィックの流れは基本的に同じですが、SurfinGate プラグインは AIX ファイアウォールでは使用できません。このため、SurfinGate サーバーは、クライアントからファイアウォールへのプロキシー・チェーンの中の 1 つのプロキシーとしてセットアップされる必要があります。要求を、ファイアウォール HTTP プロキシーに直接転送するのではなく、 SurfinGate サーバーに転送するよう、WEBsweeper をセットアップする必要があります。さらに SurfinGate サーバーは、要求をファイアウォール HTTP プロキシーに転送するように構成されている必要があります。 SurfinGate サーバーではグループ情報が使用できないため、ポリシーの判断は、IP アドレスに基づいてしか行うことができません。

メールの例: MAILsweeper は、メール・ゲートウェイとしてセットアップされます。MAILsweeper サーバーに到着したメールは、次のメール・サーバーに転送される前にそのコンテンツのフィルター処理が行われます。

セキュア・メール・サーバーのそれぞれは、クライアントのメール要求を MAILsweeper サーバーに転送するよう構成されている必要があります。着信するメールを MAILsweeper サーバーに転送するために、ファイアウォールのメール交換機能が構成されている必要があります。

MAILsweeper は、いずれの外部ドメインにアドレス指定されたメールも、ファイアウォールのメール交換機能に送信するように構成されている必要があります。 MAILsweeper は、内部ドメインにアドレス指定されたメールを、正しいセキュア・メール・サーバーに送信するように構成されている必要があります。

第2章 IBM の SecureWay Boundary Server の紹介

この章では、SecureWay Boundary Server の概要を説明しますが、以下の節が含まれています。

- 『SecureWay Boundary Server とは何か』
- 『SecureWay Boundary Server がなぜ必要か』
- 6ページの『SecureWay Boundary Server がどのようにして FirstSecure に組み込まれているか』
- 6ページの『SecureWay Boundary Server の構成要素は何か』

SecureWay Boundary Server とは何か

IBM SecureWay Boundary Server は、初めて、完全な境界セキュリティーのソリューションを 1 つにまとめたものです。 SecureWay Boundary Server は、ファイアウォール保護、仮想私設網 (VPN)、およびコンテンツ・セキュリティーを提供します。
SecureWay Boundary Server は、セキュリティー産業からのテクノロジーを 1 つにまとめて、 IBM のサポートとその背後にあるサービスを一緒にして、統合されたソリューションにしたものです。このソリューションには、以下のものが含まれています。

- IBM SecureWay Firewall 4.1 (Security Dynamic ACE/Server を含む)
- Content Technologies の MIMEsweeper
  - MAILsweeper 4.1_2
  - WEBsweeper 3.2_5
  - WEBsweeper HTTPS proxy 1.0_2
- Finjan の SurfinGate 4.05
  - SurfinGate サーバー
  - SurfinConsole
  - SurfinGate データベース
  - SurfinGate Plugin for WTE integration for Windows NT 1.0

SecureWay Boundary Server がなぜ必要か

セキュア境界がどこにでも (技術部門と人事部門などの部門の間、本社ネットワークとリモート・オフィスの間、社内ネットワークとインターネットの間、社内の Web アプリケーションと顧客の間、および社内ネットワークまたはアプリケーションとビジネス・パートナーの間に) 必要です。境界セキュリティーは、使用しているネットワーク、アプリケーション、および情報などを保護するだけではなく、それらの有効範囲も広げます。境界セキュリティーを適切にするためには、そのネットワークをアクセスできる人とネットワークに出入りする情報の両方を制御する必要があります。

SecureWay Boundary Server がどのようにして FirstSecure に組み込まれているか

IBM SecureWay FirstSecure は、1 つの統合製品のパッケージです。これは、インターネットやその他のネットワークを介した、ネットワーキングのすべての面の機密保護を援助するために、包括的なフレームワークを提供します。これは、モジュール形式で、相互操作が可能なオファリングを使用して、セキュア e-business を行うために、現在の投資をもとに計画を作成し、所有者にかかる合計コストを最小限にするために役立ちます。これは、ウィルス保護、アクセス制御、トラフィック・コンテンツの制御、暗号化、ディジタル証明書、ファイアウォール、ツールキット、および導入サービスを提供します。

Boundary Server は、FirstSecure に入っている製品パッケージの 1 つです。これはインターネットに対して境界を作成するので、これを使用して、有害の可能性のあるウィルス (付随するウィルス・スキャン製品を使用して) ブロックし、 JavaScript、Java アプレット、ActiveX コントロール、およびジャンク E メール (SPAM) さえもブロックすることができます。 Boundary Server を使用して、インターネットから自分のネットワークに入力したいものを正確に制御します。 SecureWay Policy Director を使用して、ファイアウォール・プロキシー・ユーザーと、それらのユーザーの認証ポリシーを管理します。

SecureWay Boundary Server の構成要素は何か

SecureWay Boundary Server の 3 つの構成要素は、IBM Firewall、MIMEsweeper、および SurfinGate からなっています。 SecureWay Boundary Server は、 IBM SecureWay Policy Director との統合を提供します。

IBM SecureWay Boundary Server の概要

IBM SecureWay Boundary Server は、大規模組織に対して、顧客、サプライヤー、およびパートナーに対して自分の企業を安全に開放することで e-business を活用するために必要な、保護、アクセス制御、およびコンテンツ・セキュリティーを提供します。この機能には、以下のものがあります。

- ネットワークに対するファイアウォールによる保護
- ネットワークの到達度を拡張する仮想私設網 (VPN)
- 企業のデータ、イメージ、および義務と生産性を保護するための、電子メールと Web トラフィックのコンテンツ・スキャナー

SecureWay Boundary Server は、産業からの最高のテクノロジーを 1 つにまとめて、IBM のサポートとその背後にあるサービスを一緒にして、統合されたソリューションにしたものです。これは、AIX と Windows NT のオペレーティング・システムで使用可能です。

SecureWay Boundary Server の機能

SecureWay Boundary Server は、ネットワークとシステムを隠して保護するために、パケットのフィルター処理、プロキシー、および Socks サーバーのテクノロジーと、コンテンツ・セキュリティーを適用しています。これらのテクノロジーにより、管理者は、どのデータをネットワークに出入りさせて渡せるかを明示して定義することができます。これは、「サービス否定のハッキング」を防止し、ハッカーがネットワークに入り込み、法的責任に制限を加えるのを防止するのに役立ちます。 SecureWay Boundary Server は、VPN ソリューションを提供して、リモート・サーバーとモデムのバンクをインターネット・ベースのソリューションに置き換えることができます。

Policy Director と一緒に配置された場合、SecureWay Boundary Server は、中央のポリシー・ベースの仕組みを使用して、ユーザーの認証を提供します。アンチウィルス・ソフトウェアを SecureWay Boundary Server と一緒に使用して、サイトのウィルス保護を提供することができます。

IBM SecureWay Policy Director の概要

Policy Director は、許可とセキュリティー管理を提供する独立型ソリューションであり、地理的に分散したイントラネットとエクストラネット上に存在するリソースについて、終端から終端までの機密保護を提供します。エクストラネットは、アクセス制御とセキュリティー機能を使用して、インターネットに接続された 1 つまたは複数のイントラネットの使用を、選択された加入者に制限する仮想私設網 (VPN) です。 Policy Director は、認証、許可、データ・セキュリティー、およびリソース管理のサービスを提供します。 Policy Director を標準のインターネット・ベース・アプリケーションと一緒に使用すると、機密保護され、管理の行き届いたイントラネットとエクストラネットを構築できます。

IBM SecureWay Policy Director の機能

SecureWay Boundary Server と一緒に使用した場合、IBM SecureWay Policy Director は、プロキシー・ユーザー・ポリシーの保管場所と、認証情報を提供します。

IBM SecureWay Firewall の概要

IBM SecureWay Firewall は、ネットワーク・セキュリティー・プログラムです。ファイアウォールは、1 つまたは複数の機密保護された内部の私設ネットワークと、他のネットワークまたはインターネットとの間を遮断するものです。ファイアウォールは、セキュア・ネットワークの中へ、または外への希望しないか、または無許可の通信を防止します。

IBM SecureWay Firewall の機能

IBM SecureWay Firewall は、保護されたネットワーク、インターネット、および他のネットワークのセットの間のアクセスを制限します。また、以下のことも行います。

- 周到に制御された地点に人が入るのを制限する
- ハッカーが他の防御設備に近づくのを防止する

- 周到に制御された地点から人が出ていくのを制限する
- 内部ファイアウォールで、内部の機密情報を無許可の従業員から隔離する
- ネットワークを出入りすることができるトラフィックを制限する

MIMEsweeper の概要

MIMEsweeper は、電子メールまたはワールド・ワイド・ウェブ (WWW) 経由のファイアウォールを通して渡されるデータを分析することによって、コンテンツ・セキュリティーを提供します。コンテンツ・セキュリティーによって、組織は、電子メールやワールド・ワイド・ウェブ (WWW) の使用に関連するビジネス上の問題点を効率的に管理することができます。これらの問題点は、ネットワークの保全性とビジネスの保全性に分けることができます。

ネットワークの保全性のためのフィルター処理によって、以下のことが可能になります。

- 着信および発信する電子メールのウィルスを識別して除去する
- 望ましくないファイル・タイプをフィルターに掛ける
- サイズ超過のファイルを管理する
- メール爆弾によるハッキングからの輻輳 (ふくそう) またはサービスの低下からネットワークを保護する

ビジネスの保全性のためのフィルター処理によって、以下のことが可能になります。

- 機密性の侵害および商取引上の秘密の漏えいを防止する
- 法的義務の公開を制限する
- 従業員による電子メールおよびワールド・ワイド・ウェブ (WWW) の誤用による損失を低減する
- 誤用または敵意のあるハッキングによるネットワーク・サービスの損失を防ぐ

ネットワークの保全性に対する脅威には、データの破壊または消去、電子メールの混乱、およびシステム・ハードウェアの破壊が考えられますが、これらのすべてが、ネットワークのダウン時間となり、生産性の低下を招き、そのクリーンアップと回復のために高いコストがかかることになります。

しかし、ビジネスの保全性に対する脅威は、法律に関する膨大なコスト、知的所有権の逸失、および企業の評判や信頼性に対する損傷によって、もっと破壊的なものになり得ます。ビジネスの保全性の問題は、取り引きの運営を行き詰まらせる可能性もあります。

MIMEsweeper は、電子メールやインターネットを組織で使用することによって提起される、ネットワークとビジネスの保全性の問題から組織を保護するための、産業界でも先進的な製品です。

MIMEsweeper の機能

MIMEsweeper は、以下のことができます。

- 発信されるメールに法律的な断わり書きを追加する
- 機密性のある文書およびデータを保護する
- 電子メールおよび Web ベースのユーザーの許可と制御を行う
- 攻撃的なデータを隔離またはブロックする
- ジャンク電子メールをブロックする
- 該当するコンテンツの添付物およびダウンロードをスキャンする
- ウィルスや悪意を持ったコードを停止する
- 不適切な Web ページやサイトをブロックする
- 報告、ログ、およびアーカイブを行う

SurfinGate の概要

SurfinGate 4.05 は、商取引にインターネット、エクストラネット、またはイントラネットを使用しているビジネスのための、モバイル・コードのセキュリティー・ツールです。 JavaScript に含まれているモバイル・コードのコンテンツ検査を通して、SurfinGate は、産業スパイ、データの改ざん、および情報の削除などを含む、敵意のある損傷または意図的でない損傷からコンピューター・ネットワークを保護するのを援助します。 SurfinGate のコンテンツ検査プロセスは、ゲートウェイ・レベルで Java、JavaScript、および ActiveX のモバイル・コードの内容を検査して、重要なリソースから遠ざけるようにし、コードに固有の ID とアプレット・セキュリティー・プロファイル (ASP) を割り当てて、セキュリティーの侵害の可能性があることを通知します。SurfinGate は、疑わしいと思われるコードを、ネットワークに入る前に識別します。

SurfinGate 4.05 には、以下の 4 つの構成要素が含まれています。

- SurfinGate サーバー
- SurfinConsole
- SurfinGate データベース
- SurfinGate Plugin for WTE integration for Windows NT

SurfinGate Server は、HTTP プロキシー・サーバーとして働きます。 SurfinGate は、ファイアウォール HTTP プロキシーおよび WEBsweeper プロキシーと一緒のプロキシー・チェーンの一部として配置することができます。 Windows NT の場合、ファイアウォール HTTP プロキシーのプラグインの代替として使用できます。プラグインとして使用された場合、SurfinGate は、要求を行っているプロキシー・ユーザーについてのグループ情報を入手します。 SurfinGate のフィルター処理のポリシーは、このグループ情報に基づいたものにすることができます。このアーキテクチャーによって、モバイル・コードのトラフィックを停止させ、ハッキングが発生する前に検査することができます。この構成要素は、企業セキュリティー・ポリシーに従った保護を提供します。

SurfinConsole は、モバイル・コードに対する中央の企業セキュリティー・ポリシーの管理と設定を行うための使いやすいインターフェースです。 SurfinConsole は、ネットワーク上の複数の SurfinGate Server を制御することができ、ユーザーごとまたはグループごとに、あるいは受け入れ可能でないコードと受け入れ可能なコードについてのカスタム・リストによって、企業全体でのモバイル・コードに関する規則を強制することができます。

SurfinGate データベースは、ユーザーとグループに関する情報およびそれらの対応するセキュリティー・ポリシーが入っている、アプレット・セキュリティー・プロファイル (ASP) の詳細を保管します。このデータベースは、組み込みのアクセス・データベース・エンジンまたは既存の Oracle データベースを使用することができます。 SurfinGate がすべてのモバイル・コードの内容を実行中に検査しているので、このデータベースはセキュリティーのためには必要ありませんが、大規模の操作ではパフォーマンスを向上させるのに役立ちます。

SurfinGate の機能

SurfinGate は、以下のものを提供します。

- Java アプレット、Active X コントロール、JavaScript 用のゲートウェイ・レベルのコンテンツ検査サーバー
- リアルタイム監視、動的検査
- Web ベースのモバイル・コードに対するセキュリティー・ポリシーの強制
- 「モバイル・コード」(たとえば、Java アプレット、ActiveX コントロール、JavaScript, Visual Basic スクリプト、プラグイン、cookie) の検査

SurfinGate は、プロキシー・チェーンの中のプロキシーと一緒に働くか、または Windows NT 用の Firewall 上の WTE プラグインを介して働きます。

第3章 SecureWay Boundary Server をインストールする前に

本章では、SecureWay Boundary Server のインストールの準備を行う方法について説明し、以下の節が含まれています。

- 『準備を行う方法』
- 13ページの『SecureWay Boundary Server』

準備を行う方法

この節では、SecureWay Boundary Server の構成要素を準備する方法について説明します。

SecureWay Policy Director との統合

Windows NT または AIX での IBM SecureWay Policy Director の基本的なセットアップについては、以下を行います。

1. オペレーティング・システムが Policy Director をサポートするように正しく構成されていることを検査する。
2. どのサーバー構成要素が配置の要件に最もよく適合しているか、およびこれらの構成要素をどのマシンにインストールするかを決定する。
3. DCE インフラストラクチャーが存在していない場合は、それをインストールして、構成する。
4. SecureWay Directory (LDAP) をインストールして、構成する。
5. クライアント証明書の認証を行う予定である場合は、 Certificate Authorization Service (CAS) を構成する。
6. NetSEAT クライアントをインストールする。
7. Policy Director サーバー構成要素をインストールする。
8. 管理コンソールをインストールする。

Policy Director についての詳細は、*Policy Director 概説 バージョン 3.0* を参照してください。

SecureWay Firewall

Windows NT または AIX での IBM Firewall の基本的なセットアップは、以下を行います。

1. 17ページの『SecureWay Boundary Server のハードウェア要件』にリストされている前提条件が揃っているか確認する。
2. IBM Firewall のセットアップの計画を立てる。前もって、ファイアウォールのどの機能が必要で、どのような方法で使用したいかを決めておきます。

3. どのインターフェースがセキュア・ネットワークに接続されるかを Firewall に指示する。自分のファイアウォールが正しく作動するためには、セキュア・インターフェースと非セキュア・インターフェースがなければなりません。構成クライアントのナビゲーション・ツリーから、 「System Administration」フォルダーを開き、「**Interfaces**」をクリックして、自分のファイアウォール上のネットワーク・インターフェースのリストを調べます。インターフェースのセキュリティー状況を変更するには、1 つのインターフェースを選択して、**Change** をクリックします。

   注: インターネットに接続しようとしている場合は、インターネット・サービス・プロバイダー (ISP) に連絡して、Firewall 非セキュア・インターフェースのための登録済み IP アドレスを入手してください。

4. 「System Administration」フォルダーの中の「**Security Policy**」ダイアログをアクセスして、一般的なセキュリティー・ポリシーをセットアップする。典型的な Firewall 構成では、以下のとおりです。
   - DNS 照会を許可する
   - 非セキュア・インターフェースへの同報通信メッセージを拒否する
   - 非セキュア・アダプターへの Socks を拒否する
5. ドメイン・ネーム・サービスとメール・サービスをセットアップする。 DNS レゾリューションを提供しないと、効率的な通信は行われません。これらの機能は、構成クライアントのナビゲーション・ツリーにある「System Administration」フォルダーからアクセスします。
6. 構成クライアントのナビゲーション・ツリーの中の「**Network Objects**」機能を使用して、ネットワークの主要な要素をファイアウォールに定義する。「Network Objects」は、Firewall を介したトラフィックを制御します。以下の主要な要素をネットワーク・オブジェクトとして定義します。
   - Firewall のセキュア・インターフェース
   - Firewall の非セキュア・インターフェース
   - セキュア・ネットワーク
   - 使用しているセキュア・ネットワーク上にある各サブネット
   - 使用している Security Dynamics サーバーおよび Windows NT のドメイン・サーバーのためのホスト・ネットワーク・オブジェクト (該当する場合)
7. Firewall 上のサービスを使用可能にする。これらは、(socks またはプロキシーなどの) メソッドであり、それによって、セキュア・ネットワーク内のユーザーは非セキュア・ネットワークをアクセスできます。どのサービスを導入するかは、計画段階で行った決定によります。一部の接続構成で特定のタイプのトラフィックをセットアップする場合には、導入サービスが必要になる場合があります。たとえば、自社のセキュア・ユーザーが、HTTP プロキシーを用いて、インターネット上のウェブをサーフィンするのを許すとすれば、管理者は、 HTTP プロキシー・デーモンをファイアウォールに構成する必要があるばかりでなく、 HTTP トラフィックを許すような接続を設定することも必要になります。 Policy Director をセットアップする場合には、11ページの『SecureWay Policy Director との統合』を参照してください。

8. **Windows NT のみ:** 強化プロセスが NETBIOS を使用不可にするため、認証に Windows NT ドメイン・パスワードを使用したい場合は、認証用のトラステッド Windows NT ドメインを検索する機能を装備した、Windows クライアント・コードを構成する必要があります。トラステッド Windows NT サーバーは、TCP/IP ホスト名とアドレスを持っている必要があり、またそのサーバーと Firewall との間の TCP/IP 接続を持っている必要があります。ファイアウォール管理者は、Firewall とトラステッド Windows NT サーバーの間に接続を作成して、その 2 つの間のトラフィックを可能にする必要があります。
9. ネットワーク・アドレス変換を使用する予定である場合、まず最初に、ISP に連絡して、多対 1 のアドレス変換に使用する登録済み IP アドレスを取得する。このアドレスは、ステップ 12ページの3 で要求したアドレスに追加されるものです。次に、「*Add NAT Configuration*」パネルで、その登録済み IP アドレスを「*Many-to-One IP Address*」フィールドに追加します。

上記のステップは、基本ファイアウォール構成を立ち上げて、実行するのに役立つはずです。 IBM Firewall は、ネットワークのセキュリティーを確実なものにするのを援助するために、システム・ログなどの他の機能を提供しています。

Firewall が正常または異常のいずれかでシャットダウンした場合でも、構成データは、ハード・ディスクに保管され、リブート時に自動的に再活動化されるので、影響を受けることはありません。ただし、たとえばアクティブ FTP セッションなど、一部のアクティブ接続が中断されると、特定のファイアウォール・ログ・メッセージが発生します。

SecureWay Boundary Server

SecureWay Boundary Server ウィザードを使用して、Policy Director と統合するために、ユーザーの管理用の IBM SecureWay Policy Director を使用するよう Firewall をセットアップすることができます。任意選択で、このウィザードはファイアウォール HTTP プロキシーを構成して、認証情報を SurfinGate プラグインに渡します (Windows NT のみ)。

Firewall 用の IBM SecureWay Boundary Server を構成するために必要な情報は、以下のとおりです。

- Firewall が使用する IBM SecureWay Directory サーバーのホスト名とドメイン。
- IBM SecureWay Directory サーバーが聴取するポートの数。デフォルトのポート数は 389 です。
- IBM SecureWay Directory サーバー用の SecurityMaster パスワード。
- この Firewall に対するプロキシー・ユーザーを区別するために使用するドメイン名。この名前を使用するすべてのファイアウォールが、同じユーザーのセットを管理します。通常、Firewall マシンの完全修飾ホスト名を使用します。
- SecureWay Directory の中に保管されたプロキシー・ユーザーをアクセスするために使用される Firewall 管理者名。この名前には、SecureWay Policy Director で作成された

すべてのプロキシー・ユーザーを変更するためのアクセス権が許可されます。
Firewall マシンの完全修飾ホスト名を使用する必要があります。

- IBM SecureWay Directory が、データベース内の Firewall ユーザーの検索を開始するルートとして使用する識別名。これは、Policy Director ユーザーを保管するために SecureWay Directory 内に作成したサフィックスである必要があります。
- IBM SecureWay Directory サーバーに接続するときに使用するための、Firewall の管理者 ID のためのパスワード。

Firewall と the SecureWay Directory サーバーとの間でトラフィックが流れるようにするために、接続を作成する必要があります。

17ページの『SecureWay Boundary Server のハードウェア要件』にリストされている前提条件が揃っているか確認してください。

SurfinGate

SurfinGate を使用する準備をするためには、Windows NT Service Pack 5 がインストールされている必要があります。 17ページの『SecureWay Boundary Server のハードウェア要件』にリストされている前提条件が揃っているか確認してください。

SurfinGate を使用する準備のために、以下を実行してください。

- Oracle データベースを使用している場合は、それを構成する必要があります。
- Windows NT Firewall を使用している場合は、プラグインまたはプロキシー・モードを使用するかどうか決定する必要があります。
- WTE で SurfinGate プラグインを使用可能にするには、 Firewall マシンに SurfinGate プラグインをインストールして、 SecureWay Boundary Server ウィザードを実行します。
- SurfinGate プラグインから SurfinGate サーバーへのトラフィックが流れるようにするために、接続を作成する必要があります。

MIMEsweeper

MIMEsweeper の使用の準備をするためには、ネットワークをどのように動作させようとしているかを理解している必要があります。 17ページの『SecureWay Boundary Server のハードウェア要件』にリストされている前提条件が揃っているか確認してください。

MAILsweeper

MIMEsweeper を構成する場合は、MAILsweeper と WEBsweeper を別々のマシンに入れる必要があります。

MAILsweeper を構成する前に、以下の作業を実行してください。

- 内部で使用するメール・ドメインを判別する。 MAILsweeper と Firewall メール交換機能は、これらの各メール・ドメインのメールを受け入れるよう構成される必要があります。
- どのセキュア・メール・サーバーが、各ドメインをサポートするかを判別する。MAILsweeper は、すべてのメール・ドメインにアドレス指定されたメールが、正しいメール・サーバーに転送されるように構成されている必要があります。
- MAILsweeper サーバーのアドレスを判別する。セキュア・メール・サーバーのそれぞれは、内部クライアントから受信したメールを MAILsweeper サーバーに転送するよう構成されている必要があります。
- Firewall のアドレスを判別する。 MAILsweeper は、外部ドメインにアドレス指定されたメールを Firewall メール交換機能に転送するよう構成されている必要があります。

WEBsweeper

WEBsweeper を構成する前に、以下の作業を実行してください。

- WEBsweeper サーバーのアドレスを判別する。これは、ネットワーク内の各クライアント Web ブラウザーごとに必要です。ブラウザーは、HTTP、FTP、および HTTPS のためのプロキシーとして WEBsweeper サーバーを使用するよう構成されている必要があります。
- 自分のファイアウォールのセキュア・インターフェースのアドレスを判別する。WEBsweeper は、プロキシー要求を Firewall に常駐する HTTP プロキシーに転送するよう構成されている必要があります。
- クライアントが Web コンテンツのフィルター処理をう回できるようにしたくない場合は、Firewall 上の接続をセットアップして、WEBsweeper か SurfinGate サーバー、あるいはその両方に対するプロキシー・アクセスを制限するようにする必要があります。

第4章 IBM SecureWay Boundary Server (SBS) の要件

この章では、SecureWay Boundary Server の最小必要条件を示します。

SecureWay Boundary Server のハードウェア要件

Boundary Server 構成要素製品のハードウェア要件を以下の表に示します。

表 2. Boundary Server 構成要素製品のハードウェア要件

Boundary Server 構成要素	マシン・タイプ	ディスク・スペース	メモリー	その他
Policy Director	N/A	64 MB	16 MB	N/A
IBM Firewall	• Windows NT: 266 MHz 以上 • AIX: 4.3.2 をサポートする RS/6000 マシン	Windows NT: 200 MB AIX: 200 MB	Windows NT: 64 MB AIX: 128 MB	ネットワーク・インターフェース・カード (NIC) 2 枚
ACE/Server	• Windows NT: 166 MHz 以上 (シングル・プロセッサーのみ) • AIX: AIX 4.2 をサポートするマシン	• 1 次サーバー・ソフトウェア: 50 MB • バックアップ・サーバー: 22MB • 初期ユーザー・データベース: 4 MB • インストール: 240 MB	最小: 32 MB	実際の記憶域要件は、ユーザー数によって決まる。
MAILsweeper	Windows NT: 400 MHz プロセッサー以上	1 GB	128 MB	N/A
WEBsweeper	Windows NT: 450 MHz プロセッサー以上	1 GB	128 MB	N/A
大容量環境における WEBsweeper システムの要件	Windows NT: 450 MHz プロセッサー以上	3 GB	512 MB	N/A
SurfinGate 4.05 サーバー	Windows NT: 233 MHz プロセッサー以上	20 MB	256 MB	N/A

表 2. Boundary Server 構成要素製品のハードウェア要件 (続き)

SurfinGate 4.05 コンソール	Windows NT: 233 MHz プロセッサー以上	15 MB	64 MB	N/A

注: 複数言語についての詳細は、 IBM SecureWay Firewall for AIX または Windows NT バーションのセットアップとインストールに関する資料を参照してください。 Netscape ブラウザーの場合、138 MB のディスク・スペースも必要です。

SecureWay Boundary Server のソフトウェア要件

Boundary Server 構成要素製品のソフトウェア要件を以下の表に示します。

表 3. Boundary Server 構成要素製品のソフトウェア要件

製品	Windows	AIX	その他
Policy Director サーバー	Windows NT バージョン 4.0 (Service Pack 5 付き)	4.3.1	N/A
IBM Firewall	Windows NT バージョン 4.0 (Service Pack 5 付き)	4.3.2	N/A
SecureWay Boundary Server	IBM SecureWay Firewall 4.1	IBM SecureWay Firewall 4.1	N/A
MAILsweeper	Windows NT バージョン 4.0 (Service Pack 5 付き); Internet Explorer 4.01 以上; Microsoft Management Console 1.1; NTFS ドライブ; Windows Messaging	N/A	使用したいアンチウィルス・ツール
WEBsweeper	Windows NT バージョン 4.0 (Service Pack 5 付き)	N/A	使用したいアンチウィルス・ツール
SurfinGate サーバー	Windows NT バージョン 4.0 (Service Pack 5 付き)	N/A	N/A
SurfinGate 4.05 コンソール	Windows NT バージョン 4.0 (Service Pack 5 付き) または Windows 95	N/A	N/A

第5章 SecureWay Boundary Server のインストールおよび構成

この章では、Windows NT および AIX での SecureWay Boundary Server の構成とインストールの方法について説明します。

- 『SecureWay Boundary Server 構成要素のインストール』
- 21ページの『SecureWay Boundary Server 構成要素の構成』
- 30ページの『割り込みのブロッキング』

SecureWay Boundary Server 構成要素のインストール

この節は、Windows NT および AIX 版の IBM SecureWay Firewall、SurfinGate、および MIMEsweeper をインストールするのに役立ちます。

SecureWay Firewall のインストール

IBM SecureWay Firewall for Windows NT and AIX の基本構成についての詳細は、11ページの『準備を行う方法』を参照してください。そこでは、セキュア・インターフェースの定義方法、セキュリティー・ポリシーの決定方法、およびネットワーク・オブジェクトの定義方法について説明しています。 SecureWay Firewall についての詳細は、*IBM SecureWay Firewall for AIX セットアップおよびインストールの手引き* および *IBM SecureWay Firewall for Windows NT セットアップおよびインストールの手引き* を参照してください。

SecureWay Directory のインストール

SecureWay Boundary Server の LDAP 機能を使用している場合は、*IBM SecureWay Policy Director 概説 バージョン 3.0* を参照してください。

SecureWay Directory サーバーは、Firewall のセキュア・サイドか、または Firewall のセキュア非武装地帯 (DMZ) 内に存在しなければなりません。

SecureWay Policy Director のインストール

SecureWay Boundary Server の LDAP 機能を使用している場合は、SecureWay Policy Director をインストールする必要があります (*IBM SecureWay Policy Director 概説 バージョン 3.0* を参照)。

SecureWay Boundary Server のインストール

SecureWay Boundary Server を Windows NT にインストールするには、以下を行います。

- SecureWay Firewall for Windows NT をインストールする
- SecureWay Boundary Server CD から setup.exe を実行する

- 言語を選択して「**OK**」をクリックする
- InstallShield が、SecureWay Boundary Server をどこへインストールしたいかを尋ねてきます。 Windows NT のデフォルト・ディレクトリーは C:¥Program Files¥IBM¥SBS です。
- リブートする

SecureWay Boundary Server を AIX にインストールするには、以下を行います。

- SecureWay Firewall for AIX をインストールする
- CD を挿入して、SMITTY を使用してインストールする
- 「Software Installation and Maintenance」を選択する
- 「Install and Update Software」を選択する
- 「Latest Available Software」から「Install and Update」を選択する
- INPUT デバイスを尋ねてきた場合、選択項目をリストして、CD-ROM ドライブを選択する
- インストールする SOFTWARE の選択項目をリストして、sbs を選択する
- 「**Enter**」を押して、ソフトウェアをインストールする
- リブートする

SurfinGate のインストール

SurfinGate には、SurfinGate サーバーと SurfinGate コンソールの 2 つの構成要素があります。 SurfinGate のいずれかの構成要素をインストールするには、 SurfinGate CD の `¥docs¥install.pdf` に入っているインストール・ガイドを参照してください。

SurfinGate プラグイン

IBM SecureWay Firewall For Windows NT に SurfinGate プラグインをインストールするには、 SurfinGate CD の `¥docs` ディレクトリーに入っているインストール・ガイドを参照してください。

MIMEsweeper のインストール

MIMEsweeper には、MAILsweeper、WEBsweeper、および WEBsweeper HTTPS という 3 つの構成要素があります。

: MAILsweeper 4.1 は、NTFS 区画にインストールされる必要があります。

MAILsweeper のインストール

MAILsweeper をインストールするには、MIMEsweeper CD の `¥install¥MSW4_0_2¥docs¥qsg.pdf` にある、*Getting Started Guide* を参照してください。

MAILsweeper は、WEBsweeper HTTP プロキシーと同じマシンにはインストール**しないでください**。

MAILsweeper は、WEBsweeper HTTPS プロキシーと同じマシンにはインストール**しないでください**。

Windows NT CD から MAPI32.dll をインストールした後で、 MIMEsweeper CD から Microsoft Management Console 1.1 をインストールすると、正しいバージョンの MAPI32.dll が、Microsoft Management Console と一緒にインストールされた旧バージョンのもので上書きされてしまいます。 Microsoft Management Console をインストールした後、MAPI32.dll のバージョン 4.0 またはそれ以上がインストールされていることを確認してください。 dll は、通常 Windows Messaging 構成要素の中にあります。

WEBsweeper のインストール

WEBsweeper をインストールするには、MIMEsweeper CD の ¥install¥WSW3_2_5¥docs¥manual.pdf にある *Administrator's Guide* を参照してください。

: WEBsweeper は、MAILsweeper と同じマシンにはインストール**しないでください**。

WEBsweeper HTTPS のインストール

WEBsweeper HTTPS をインストールするには、MIMEsweeper CD の ¥install¥WSWHTTPS1_0_2¥readme.txt にある *Readme* を参照してください。

WEBsweeper HTTPS プロキシーは、MAILsweeper と同じマシンにはインストール**しないでください**。

SecureWay Boundary Server 構成要素の構成

SecureWay Firewall の構成

IBM Firewall の基本的なセットアップは、以下を行います。

1. IBM Firewall のセットアップの計画を立てる。前もって、Firewall のどの機能が必要で、どのような方法で使用したいかを決めておきます。
2. どのインターフェースがセキュア・ネットワークに接続されるかを Firewall に指示する。自分のファイアウォールが正しく作動するためには、セキュア・インターフェースと非セキュア・インターフェースがなければなりません。構成クライアントのナビゲーション・ツリーから、 「System Administration」フォルダーを開き、「**Interfaces**」をクリックして、自分のファイアウォール上のネットワーク・インターフェースのリストを調べます。インターフェースのセキュリティー状況を変更するには、1 つのインターフェースを選択して、「**Change**」をクリックします。
3. 「System Administration」フォルダーの中の「**Security Policy**」ダイアログをアクセスして、一般的なセキュリティー・ポリシーをセットアップする。典型的な Firewall 構成は、以下のとおりです。
   - DNS 照会を許可する

- 非セキュア・インターフェースへの同報通信メッセージを拒否する
- 非セキュア・アダプターへの Socks を拒否する

4. ドメイン・ネーム・サービスとメール・サービスをセットアップする。 DNS レゾリューションを提供しないと、効率的な通信は行われません。これらの機能は、構成クライアントのナビゲーション・ツリーにある「System Administration」フォルダーからアクセスします。
5. 構成クライアントのナビゲーション・ツリーの中の「**Network Objects**」機能を使用して、ネットワークの主要な要素を Firewall に定義する。「Network Objects」は、Firewall を介したトラフィックを制御します。以下の主要な要素をネットワーク・オブジェクトとして定義します。
   - Firewall のセキュア・インターフェース
   - Firewall の非セキュア・インターフェース
   - セキュア・ネットワーク
   - 使用しているセキュア・ネットワーク上にある各サブネット
   - 使用している Security Dynamics サーバーおよび Windows NT のドメイン・サーバーのためのホスト・ネットワーク・オブジェクト (該当する場合)
6. Firewall 上のサービスを使用可能にする。これらは、(socks またはプロキシーなどの) メソッドであり、それによって、セキュア・ネットワーク内のユーザーは非セキュア・ネットワークをアクセスできます。どのサービスを導入するかは、計画段階で行った決定によります。一部の接続構成で特定のタイプのトラフィックをセットアップする場合には、導入サービスが必要になる場合があります。たとえば、自社のセキュア・ユーザーが、HTTP プロキシーを用いて、インターネット上のウェブをサーフィンするのを許すとすれば、管理者は、 HTTP プロキシー・デーモンをファイアウォールに構成する必要があるばかりでなく、 HTTP トラフィックを許すような接続を設定することも必要になります。
7. Firewall ユーザーをセットアップする。アウトバウンドの Web アクセスのような機能の認証、または Firewall 管理者の認証が必要な場合、それらのユーザーを Firewall に定義する必要があります。 LDAP 内のプロキシー・ユーザーを保管するために SecureWay Policy Director を使用している場合は、この時点ではプロキシー・ユーザーを作成しないでください。 Policy Director の構成時に、Policy Director コンソールを使用して Firewall プロキシー・ユーザーを作成してください。

上記のステップは、基本 Firewall 構成を立ち上げて、実行するのに役立つはずです。IBM Firewall は、ネットワークのセキュリティーを確実なものにするのを援助するために、システム・ログなどの他の機能を提供しています。

Firewall が正常または異常のいずれかでシャットダウンした場合でも、構成データは、ハード・ディスクに保管され、リブート時に自動的に再活動化されるので、影響を受けることはありません。ただし、たとえばアクティブ FTP セッションなど、一部のアクティブ接続が中断されると、特定のファイアウォール・ログ・メッセージが発生します。

Policy Director の統合のための SecureWay Firewall の構成

Policy Director との統合を利用するためには、Firewall は、SecureWay Boundary Server ウィザードと一緒に IBM SecureWay Policy Director を使用するように構成されている必要があります。 IBM SecureWay Policy Director が使用されない場合、プロキシー・ユーザーは、Firewall グラフィカル・ユーザー・インターフェース (GUI) によってのみ定義されます。そのようなユーザーは、SecureWay Policy Director では管理できません。

SecureWay Firewall が SecureWay Directory と対話を行えるようにするには、接続を作成する必要があります。 SecureWay Directory は、Firewall のセキュア・サイド (セキュア DMZ またはセキュア・ネットワークのいずれか) にある必要があります。

接続をセットアップする方法についての詳細は、*IBM SecureWay Firewall for Windows NT 使用者の手引き* および *IBM SecureWay Firewall for AIX 使用者の手引き* を参照してください。接続をセットアップするための情報は、以下のとおりです。

要求の場合、以下は、アウトバウンドの規則をセットアップするために必要な項目です。

- 送信元は Firewall のセキュア・アダプター・アドレスになる。
- 宛先は SecureWay Directory アドレスになる。
- 送信元ポートは 1023 より大きくなる。
- 宛先ポートは 389 に等しくなる。
- インターフェースは機密保護される。
- 経路指定はローカルになる。
- 方向はアウトバウンドになる。

応答の場合、以下は、インバウンドの規則をセットアップするために必要な項目です。

- 送信元は SecureWay Directory アドレスになる。
- 宛先は Firewall のセキュア・アダプター・アドレスになる。
- 送信元ポートは 389 に等しくなる。
- 宛先ポートは 1023 より大きくなる。
- インターフェースは機密保護される。
- 経路指定はローカルになる。
- 方向はインバウンドになる。

以下に接続の例を示します。

```
# Service : ldap
# Description:

permit 9.67.130.153 255.255.255.255 9.67.141.85
255.255.255.255 tcp gt 1023 eq 389 secure both
```

```
outbound l=y f=y t=0 e=none a=none

permit 9.67.141.85 255.255.255.255 9.67.130.153
255.255.255.255 tcp/ack eq 389 gt 1023 secure local
inbound l=y f=y t=0 e=none a=none
```

SecureWay Boundary Server セットアップ・ウィザードを実行します。ファイアウォールが Policy Director と一緒に作動できるようにするためのオプションを選択してください。詳しくは、26ページの『Policy Director の統合のための SecureWay Boundary Server の構成』を参照してください。

SurfinGate プラグインで使用するための SecureWay Firewall の構成 (Windows NT のみ)

SecureWay Firewall が SurfinGate サーバーと対話を行えるようにするには、接続を作成する必要があります。 SurfinGate サーバーは、Firewall のセキュア・サイドにある必要があります。

接続をセットアップする方法についての詳細は、*IBM SecureWay Firewall User's Guide for Windows NT* を参照してください。接続をセットアップするための情報は、以下のとおりです。

要求の場合、以下は、アウトバウンドの規則をセットアップするために必要な項目です。

- 送信元は Firewall のセキュア・アダプター・アドレスになる。
- 宛先は SurfinGate サーバーのアドレスになる。
- 送信元ポートは 1023 より大きくなる。
- 宛先ポートは 3141 に等しくなる。
- インターフェースは機密保護される。
- 経路指定はローカルになる。
- 方向はアウトバウンドになる。

要求の場合、以下は、インバウンドの規則をセットアップするために必要な項目です。

- 送信元は SurfinGate サーバーのアドレスになる。
- 宛先は Firewall のセキュア・アダプター・アドレスになる。
- 送信元ポートは 3141 に等しくなる。
- 宛先ポートは 1023 より大きくなる。
- インターフェースは機密保護される。
- 経路指定はローカルになる。
- 方向はインバウンドになる。

以下に、このような接続の例を示します。

```
# Service : SurfinGate Plugin Communication
# Description:

permit 9.67.143.113 255.255.255.255 9.67.143.115 255.255.255.255 tcp gt 1023 eq 3141
secure local outbound l=y f=y
permit 9.67.143.115 255.255.255.255 9.67.143.113 255.255.255.255 tcp eq 3141 gt 1023
secure local inbound  l=y f=y
```

注: 接続は同じ回線上にある必要があります。

スキャンされるデータを使用可能にするためには、SurfinGate サーバーを構成する必要もあります。 SurfinConsole (SurfinGate の管理インターフェース) では、「General」タブの下の「**Plugin Mode**」オプションにチェックを付ける必要があります。「Proxy」タブの「Next Proxy」フィールドに、Firewall の HTTP プロキシーのアドレスとポート番号を入力する必要もあります。

MAILsweeper を使用するための SecureWay Firewall の構成

SecureWay Firewall に定義された Mail Exchanger は、実際のセキュア・メール・サーバーではなく、MAILsweeper マシンをポイントしている必要があります。
MAILsweeper 自体は、メールをセキュア・メール・サーバーに配達します。

SecureWay Policy Director の構成

SecureWay Directory がすでにインストールされていることを確認してください。
SecureWay Directory がインストールされているマシンのアドレス、SecureWay Directory が聴取しているポート、 SecureWay Directory サーバー上の管理者 ID、および管理者パスワードを知る必要があります。

SecureWay Directory LDAP クライアントは、SecureWay Policy Director と同じマシンにインストールしてください。(SecureWay Directory と SecureWay Policy Director 用に同じマシンを使用している場合、このクライアントがすでにインストール済みである場合があります。)

Policy Director プロキシー・ユーザーをサポートするために、 SecureWay Directory の LDAP スキーマを変更する必要があります。このスキーマの追加は、Policy Director によって提供される 2 つのファイルに保管されます。 Policy Director CD の /schema ディレクトリーにある、 secschema.def および puschema.def というファイルが必要になります。

SecureWay Directory サーバー上の LDAP スキーマを変更するには、 Policy Director マシンで、以下のコマンドを実行してください。

```
ldapmodify -h <LDAPHOST> -p <LDAPPORT>  -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f secschema.def

ldapmodify -h <LDAPHOST> -p <LDAPPORT> -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f puschema.def
```

ここで、次のとおりです。

- <LDAPHOST> は SecureWay Directory サーバーの名前です

- <LDAPPORT> はサーバーが聴取しているポートです
- <LDAPADMINUSER> は管理者 ID です
- <LDAPADMINPWD> は管理者パスワードです

プロキシー・ユーザーをサポートするよう LDAP スキーマを変更した場合、プロキシー・ユーザーが Policy Director コンソールを操作できるようにする必要があります。これを行うためには、¥Program Files¥IBM¥IVConsole ディレクトリーにある console.properties ファイルの中の Proxyusers TaskView という行がコメントになっているのを、コメントでないように変更する必要があります。

SecureWay Directory の構成

SecureWay Directory にサフィックスを定義する必要がありますが、これは、Policy Director ユーザーが保管されるルートとして使用されます。 LDAP にサフィックスを追加するには、*IBM SecureWay Directory Administrator's Guide* を参照してください。たとえば、典型的なサフィックスは、以下のようになります。

```
o=yourcompany,c=yourcountry
```

Policy Director ユーザーを保管するためのサフィックスを追加した場合、そのサフィックスをアクセス制御リスト (ACL) に正しくセットする必要があります。 Policy Director セキュリティー・グループ用の新しいサフィックスに対して、全アクセス権を提供する必要があります。 Policy Director セキュリティー・グループに対する識別名 (DN) は、以下のとおりです。

```
cn=securitygroup,secauthority=default
```

Policy Director の統合のための SecureWay Boundary Server の構成

ウィザードを使用して SecureWay Boundary サーバーの構成を行うことができます。このウィザードは、Boundary Server および Policy Director 内で、他の製品と一緒に作動する Firewall をセットアップするのに必要なステップをガイドしていきます。後に続くパネルが、LDAPサーバーに関する質問をしてきます。必要な情報をすべて入力すると、ウィザードは、Policy Director がユーザーおよびグループのポリシー用として使用しているのと同じ LDAP データベースを使用して、Firewall をセットアップします。このウィザードは、SurfinGate プラグインに認証情報を渡すために、ファイアウォール HTTP プロキシーの構成と構成解除を行うこともできます (Windows NT Firewall のみ)。

IBM SecureWay Boundary Server を構成するには、SecureWay Boundary Server ウィザードを実行します。 AIX ではコマンド **sbswizard** を実行し、 Windows NT では、「**スタート -> プログラム -> SecureWay Boundary Server**」を選択します。これによって、SBS ウィザードが立ち上げられます。

1. 「**Set up Firewall to share an LDAP database with Policy Director**」のオプションを選択します。

2. 表示される質問に、13ページの『SecureWay Boundary Server』の情報を使用して応答します。

SurfinGate プラグインを使用可能にするための SecureWay Boundary Server の構成 (Windows NT のみ)

「**スタート -> プログラム -> SecureWay Boundary Server**」を選択します。これによって、SBS ウィザードが立ち上げられます。

1. 「**Configure the Firewall HTTP Proxy to pass authentication information to the SurfinGate plugin**」のオプションを選択します。
2. ダイアログを終了します。

SurfinGate の構成

Windows NT では、以下の 2 つ方式で、SurfinGate を構成することができます。

- チェーンになったプロキシーとして
- ファイアウォール HTTP プロキシーのプラグインとして

AIX では、SurfinGate を構成する方式は以下の 1 つです。

- チェーンになったプロキシーとして

チェーンになったプロキシーとしての SurfinGate の構成

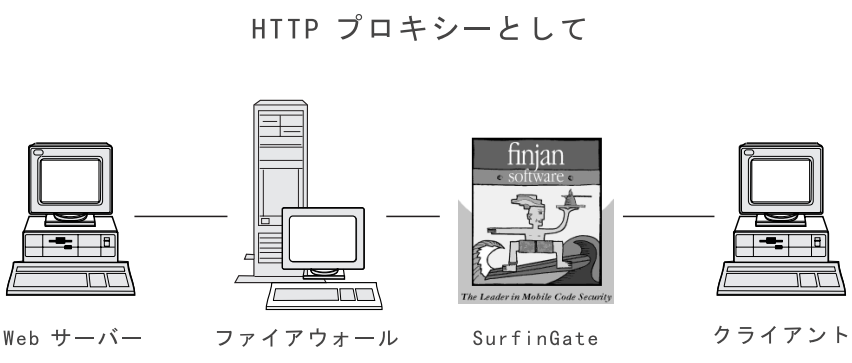


図 2. SurfinGate の構成

クライアント Web ブラウザーは、HTTP、FTP、および HTTPS のためのプロキシーとして SurfinGate を使用するように構成されている必要があります。 SurfinGate が聴取しているポート番号を必ず指定してください (デフォルトは 8080)。

SurfinConsole (SurfinGate の管理インターフェース) では、「General」タブの下の「**Proxy Mode**」オプションにチェックを付ける必要があります。「Proxy」タブの「Next Proxy」フィールドに、Firewall の HTTP プロキシーのアドレスとポート番号を

入力する必要もあります。あるいは、追加のプロキシーがすでに定義済みである場合は、次のプロキシーとして、それらのプロキシーをポイントすることができます。

ファイアウォール HTTP プロキシーのためのプラグインとしての SurfinGate の構成

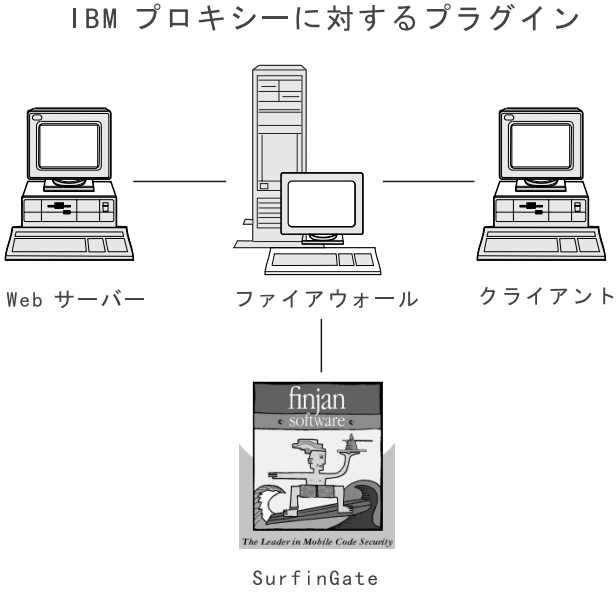


図 3. SurfinGate の構成

クライアント Web ブラウザーは、HTTP、FTP、および HTTPS のためのプロキシーとしてファイアウォール HTTP プロキシーを使用するように構成されている必要があります。ファイアウォール HTTP プロキシーが聴取しているポート番号を必ず指定してください (デフォルトは 8080)。

SurfinConsole (SurfinGate の管理インターフェース) では、「General」タブの下の「**Plugin Mode**」オプションにチェックを付ける必要があります。「Proxy」タブの「Next Proxy」フィールドに、Firewall の HTTP プロキシーのアドレスとポート番号を入力する必要もあります。

注: この機能は、SecureWay Firewall for Windows NT でのみ使用可能です。

MIMEsweeper の構成

MAILsweeper の構成

図 4. MAILsweeper の構成

環境が単純である場合は、MAILsweeper は、インストール中に尋ねられる質問によって構成する必要があります。追加の構成を行うには、SMTP コンソールで、「**スタート -> プログラム -> MAILsweeper for SMTP -> MAILsweeper**」を選択します。詳細については、*MAILsweeper Getting Started Guide* を参照してください。

WEBsweeper の構成

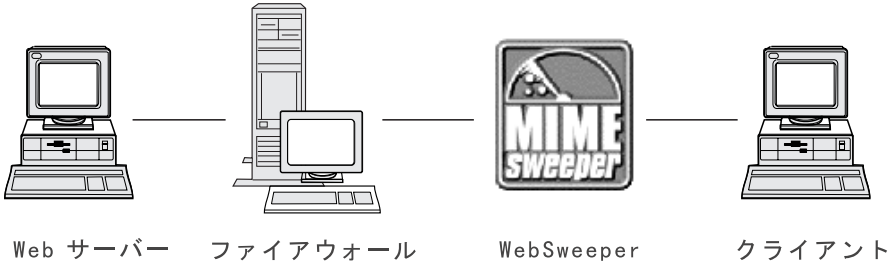


図 5. WEBsweeper の構成

構成を行うには、コントロール パネルで、WEBsweeper アプレットを選択します。詳細については、MIMEsweeper CD にある *WEBsweeper Administrator's Guide* を参照してください。

WEBsweeper HTTPS の構成

構成を行うには、コントロール パネルで、WEBsweeper HTTPS アプレットを選択します。詳細については、 *WEBsweeper Administrator's Guide* を参照してください。

割り込みのブロッキング

特定の IP アドレスをブロックすることができるフィルターを作成するためには、コマンド・ライン・ユーティリティーを使用します。ブロックするアドレスは、コンテンツ検査の結果、動的に判別することができます。このためのコマンドは、以下のとおりです。

- fwadd_deny
- fwdelete_dynamic

fwadd_deny

プログラムがパラメーターなしで起動された場合、必要なパラメーターのフォーマットを要求するプロンプトが表示されます。

パラメーターは、以下のとおりです。

フィルター ID

Windows NT Firewall の場合: 保守を編成するために、1 つの ID がフィルターに割り当てられます。 ID は 1 から始まって昇順に割り当てられます。次に使用可能な ID 番号よりも大きな ID が供給されると、割り当てられる ID は、プログラムに供給された ID 番号ではなく、次に使用可能な ID 番号になります。たとえば、ID 1 で何らかの規則が存在していて、ID 3 で 1 組のフィルター規則を作成しようとすると、代わりに ID 2 が割り当てられます。同じ ID 番号に複数の規則を割り当てることができます。規則が delete_dynamic プログラムを使用して削除されるときには、それらの規則は ID によって参照されるので、ID ごとに規則を作成するときに、同じ ID を共用している場合には、それらを 1 つのグループとして削除するものとして計画するようにしてください。

規則がすでに追加されているときには、使用された ID 番号が表示されます。

フィルター ID

AIX Firewall の場合: ID は番号で割り当てることができます。 たとえば、フィルター ID に ID 12 を指定すると、 ID=12 が割り当てられます。 AIX では、フィルターに同じ ID 番号を割り当てることはできません。各フィルターは、独自の ID を持ちます。

送信元 IP アドレス

パケットが入ってくる送信元に使用する IP アドレスは、小数点付き 10 進表記 (たとえば、255.255.255.255) で指定します。

送信元 IP マスク

このフィールドは送信元 IP アドレスと一緒に使用され、小数点付き 10 進表記で入力されます。たとえば、入力された送信元 IP アドレスが 10.5.8.0 であり、送信元 IP マスクが 255.255.255.0 である場合、10.5.8.1 から 10.5.8.255 までのすべてのパケットが対象になります。

宛先 IP アドレス

パケットの宛先に使用する IP アドレスは、小数点付き 10 進表記 (たとえば、255.255.255.255) で指定します。

宛先 IP マスク

このフィールドは宛先 IP アドレスと一緒に使用され、小数点付き 10 進表記で入力されます。たとえば、入力された宛先 IP アドレスが 10.5.8.0 であり、宛先 IP マスクが 255.255.255.0 であると、10.5.8.1 から 10.5.8.255 までのすべてのパケットが対象になります。

アダプター

アダプター指定は、以下のとおりです。

S セキュア・アダプターとして指定された場合

N 非セキュア・アダプターとして指定された場合

B すべてのアダプター (セキュアと非セキュアの両方) の場合

指定されたタイプが合致する 1 つまたは複数のアダプターから発信されたパケットは、規則に一致します。

有効範囲

ファイアウォールを介してパケットが横断する有効範囲はこのパラメーターを使用して指定され、これには、以下のいずれかの値が可能です。

L ローカル・パケットの場合

R 経路指定されたパケットの場合

B ローカル・パケットと経路指定されたパケットの両方の場合

方向 トラフィックが、インバウンド、アウトバウンド、または両方向のどちらに流れるかを指定します。

I インバウンド・トラフィックの場合

O アウトバウンド・トラフィックの場合

B インバウンドとアウトバウンドの両方のトラフィックの場合

ログ記録

動的フィルター活動に対して、ログ記録をオンにするには Y を指定し、ログ記録をオフにするには N を指定します。

fwdelete_dynamic

このプログラムがパラメーターなしで起動された場合、以下のように、現在定義されているすべての動的フィルターがリストされます。

```
>>>>  Dynamic Rule Id          =  1
 >>>>>>>>  Jump                =  0
 >>>>>>>>  Filter Action       =  Deny
```

```
>>>>>>>>  Source Address       =  9.192.8.7
>>>>>>>>  Source Mask          =  255.255.255.0
>>>>>>>>  Destination Address  =  9.192.240.1
>>>>>>>>  Destination Mask     =  255.255.255.0
>>>>>>>>  Protocol             =  Any
>>>>>>>>  Source Port          =  Any 0
>>>>>>>>  Destination Port     =  Any 0
>>>>>>>>  Adapter              =  Both (Secure and NonSecure)
>>>>>>>>  Scope                =  Both (Routed and Local)
>>>>>>>>  Direction            =  Both (Inbound and Outbound)
>>>>>>>>  Tunnel Id            =  0
>>>>>>>>  Logging Enabled      =  Unavailable
>>>>>>>>  Fragments Allowed    =  No
```

注: fwdelete_dynamic コマンドは、削除される規則が、予想された ID を持っているかどうかを最初に検査するときに使用する必要があります。

プログラムが有効なフィルター ID を使用して起動されると、動的規則が削除され、削除された規則の数が「 x Rules found with id: x」という形で表示されます。

重要: 重複してフィルターを追加しようとすると、フィルターがすでに存在していることを知らせてきます。フィルター ID を指定せずにフィルターを追加しようとすると、警告エラーを受け取ります。

AIX の割り込みブロッキングでは、上位レベルの規則セットの中に規則があると、上書きされる可能性があります。割り込みブロッキングが使用される場合、ほとんどの規則は、下位レベルの規則セットの中に入れておく必要があります。動的規則は、これらの 2 つの規則セットの中間に追加されます。上位レベルの規則の中にトラフィックを許可するものがあると、動的規則を使用してトラフィックをオフにすることができなくなります。

構成のテスト

前に説明したすべてのセットアップを終了した後、そのセットアップをテストする必要があります。 SecureWay Boundary Server の構成をテストするには、以下のようにします。

1. Policy Director を使用して Firewall Proxy ユーザーをセットアップします。セキュア Telnet 用の Firewall パスワードを使用するようにユーザーをセットし、そのユーザー用のパスワードをセットします。
2. SecureWay Boundary Server ウィザードを実行して、 Firewall と Directory (LDAP) の間のリンクを確立します。
3. セキュア・クライアントからプロキシー Telnet セッションを開始します。
4. Policy Director でユーザー・セットアップを入力します。
5. パスワードを入力するようプロンプトが出されます。
6. これで認証されました。

第6章 関連資料

本章にリストしている資料を使用すると、 IBM SecureWay Boundary Server バージョン 2.0 および関連製品の詳細を入手できます。

IBM SecureWay FirstSecure

IBM SecureWay FirstSecure 計画および統合の手引き バージョン 2.0 には、FirstSecure に関する情報が含まれています。この資料では、FirstSecure および FirstSecure を構成する製品について説明し、あらゆる IBM SecureWay 製品を使用する計画を立てる上で役に立ちます。

IBM SecureWay Firewall

以下の資料には、IBM SecureWay Firewall for Windows NT に関する情報が含まれており、IBM SecureWay Firewall CD の `x:¥books¥en_US` ディレクトリーにあり、PDF 形式と HTM 形式で使用可能です。

- *IBM SecureWay Firewall for Windows NT セットアップおよびインストールの手引き*
- *IBM SecureWay Firewall for Windows NT 使用者の手引き*
- *IBM SecureWay Firewall for Windows NT 解説書*
- *Guarding the Gates Using the IBM eNetwork Firewall for Windows NT 3.3* (レッドブック)

以下の資料には、IBM SecureWay Firewall for AIX に関する情報が含まれており、IBM SecureWay Firewall CD の `books/en_US` ディレクトリーにあり、 PDF 形式と HTM 形式で使用可能です。

- *IBM SecureWay Firewall for AIX セットアップおよびインストールの手引き*
- *IBM SecureWay Firewall for AIX 使用者の手引き*
- *IBM SecureWay Firewall for AIX 解説書*
- *A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Servers and Client Solutions* (レッドブック)

MIMEsweeper

MAILsweeper

以下の資料には、MAILsweeper に関する情報が含まれており、 MIMEsweeper CD の ¥install の下に、PDF 形式と HTM 形式で使用可能です。

- *Getting Started Guide* は ¥install¥MSW4_0_2¥Doc¥qsg.pdf にあります。

- Readme は ¥install¥MSW4_0_2¥README.htm にあります。

WEBsweeper

以下の資料には、WEBsweeper に関する情報が含まれており、 MIMEsweeper CD の ¥install の下に、PDF 形式と HTM 形式で使用可能です。

- *WEBsweeper Administrator's Guide* は ¥install¥WSW3_2_5¥Doc¥manual.pdf にあります。
- Release Note は ¥install¥WSW3_2_5¥Doc¥RELNOTES.htm にあります。

WEBsweeper HTTPS プロキシー

以下の資料には、WEBsweeper HTTPS プロキシーに関する情報が含まれており、MIMEsweeper CD の ¥install の下に、TXT 形式で使用可能です。

- Readme は ¥install¥WSWHTTPS1_0_2¥readme.txt にあります。

SurfinGate

以下の資料には、SurfinGate に関する情報が含まれており、 SurfinGate CD の ¥docs の下に、PDF 形式で使用可能です。

- *SurfinGate Installation Guide* は ¥Docs¥install.pdf にあります。
- *SurfinGate User's Manual* は ¥Docs¥manual.pdf にあります。
- Release Note は ¥Docs¥SFG 405 RelNotes.pdf にあります。
- SurfinGate プラグインに関する情報は、¥docs ディレクトリーの中にあります。

付録A. トラブルシューティング

ここでは、SecureWay Boundary Server に関連する問題の検出と解決に役立つ情報を示します。

IBM SecureWay Firewall の共通問題の解決

経路指定の問題

IBM Firewall は、「*Test IP Routing*」というタイトルの「**Security Policy**」ダイアログ・ボックスを提供しており、経路指定の問題のデバッグに便利です。このチェック・ボックスを使用可能にして、自分の接続構成を活動化して、「Connection Rules Logging」を使用可能にしてください。次に、自分のファイアウォール・ログを調べ、ファイアウォールを介して流れるすべてのパケットについての詳細情報を見てください。

これらのテストは、最初は IP アドレスを使用して行い、次にホスト名を使用して行います。

ファイアウォールからホストへの PING ができない

問題の説明

ネットワーク・インターフェースが正しく構成されていません。

推奨処置

オペレーティング・システムの資料を参照してください。

問題の説明

非セキュア・ネットワークへの接続が正しく構成されていません。

推奨処置

インターネット・サービス・プロバイダーに連絡して、援助を求めてください。

問題の説明

セキュア・ネットワークがルーターの後ろに分離されている場合、ファイアウォールはそのルーターに対する静的経路を持っている必要があります。

`netstat -rn` を使用して、静的経路指定を検査します。

```
netstat -rn
```

プロトコル・ファミリー 2 の場合、出力は以下のようになるはずです。

```
Destination  Gateway          Flags     ....
default      nrr.nrr.nrr.nrr  UG
nnn.nnn.nnn  nnn.nnn.nnn.nnn  U
sss.sss.sss  sss.sss.sss.sss  U
ss1.ss1.ss1  srr.srr.srr.srr  UG
127          127.0.0.1        U
```

図 6. netstat -rn からの出力例.

nrr.nrr.nrr.nrr
インターネットに対するルーターを表し、これがデフォルト経路になります。デフォルト経路は、静的経路 (Flag=UG) です。

nnn.nnn.nnn
非セキュア・ドメインを表します。これはインターフェース経路 (Flag=U) です。

nnn.nnn.nnn.nnn
非セキュア・インターフェースを表します。

sss.sss.sss
セキュア・ドメインを表します。これはインターフェース経路 (Flag=U) です。

sss.sss.sss.sss
セキュア・インターフェースを表します。

ss1.ss1.ss1
ネットワークのセキュア・サイドにあるサブドメインを表し、srr.srr.srr.srr は、そのサブドメインへのルーターを表します。これは、静的経路 (Flag=UG) です。

127.0.0.1
ループバックまたはローカル・ホストです。これはインターフェース経路 (Flag=U) です。

各インターフェースに対するインターフェース経路を持っている必要があり、デフォルト経路は、ファイアウォールの非セキュア・サイドのルーターをポイントしている必要があります。

推奨処置
ルーターに静的経路を追加します。ルーター管理者に連絡してください。`route add` コマンドを使用してください。

問題の説明
コンタクトを試みているセキュア・インターフェースまたはホストのサブネット・マスクが誤りである可能性があります。

推奨処置
クライアントの構成ユーティリティーを使用して、マスクの設定を訂正します。

セキュア・ホストから非セキュア・ホスト (またはその逆) への PING ができない

問題の説明

ファイアウォールに隣接する各ルーターには、ファイアウォールを越えた宛先ネットワークに対するゲートウェイとして、ファイアウォールを指定する静的経路が含まれている必要があります。

推奨処置

ルーター管理者に連絡してください。

問題の説明

セキュア・ネットワークが、RFC 1597 に指定された専用アドレスを含む、非セキュア・ネットワークに登録されていないか、経路指定可能でないアドレスを使用している場合、パケットは送信側に戻されません。

推奨処置

Windows NT の場合のみ: 登録済みのアドレスを持つクライアントを使用します。ファイアウォールの NAT フィーチャーを TCP および UDP のトラフィックに使用できますが、NAT は、PING のような ICMP パケットの中のアドレスは変換しません。

推奨処置

AIX の場合のみ: 登録済みのアドレスを持つクライアントを使用します。

DNS の障害

注: DNS は、Windows NT の場合のみです。

問題の説明

Microsoft DNS Service Manager を使用して Microsoft DNS Service を構成したため、DNS エラー・メッセージを受け取りました。

推奨処置

インストールの説明に戻って、以下を行ってください。

1. ¥winnt¥system32¥DNS ディレクトリー全体を削除することによって、Microsoft DNS を除去する
2. Microsoft DNS を再インストールする
3. リブートする
4. DNS hotfix を再インストールする
5. リブートする

共通問題の解決 - MIMEsweeper

WEBsweeper と MAILsweeper が同じマシンにあり作動しているようには見えない

問題の説明

同じマシンで MAILsweeper と WEBsweeper の実行を試みているときの問題。

推奨処置

MAILsweeper を 1 つのマシンのインストールし、WEBsweeper を別のマシンにインストールします。

WEBsweeper のパフォーマンスが低下している

問題の説明

WEBsweeper を使用しているときの Web コンテンツのダウンロードの遅れが満足できるものではありません。

推奨処置

1. WEBsweeper Control Panel アプレットを使用して、ログ記録を使用不可にする。
2. 使用可能なもっとも高速のハードウェアに WEBsweeper をインストールする。

WEBsweeper のライセンスの問題

問題の説明

WEBsweeper の以前のバージョンがインストールされていたマシンに WEBsweeper 3.2_5 をインストールしている時に、ライセンス・キーが対立する場合があります。 WEBsweeper が開始する時に、内部 Windows エラー・メッセージ: 2140 が発生する場合は、イベント・ビューアーの中のアプリケーション・ログを検査してください。 WEBsweeper からのメッセージは、「PAKMSG error: Username conflicts with previously defined license section.」です。

推奨処置

Windows レジストリーから古いライセンス・キーを除去します。 regedit をロードして、パス『¥¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Content Technologies¥MIMEsweeper¥License』の下を調べてください。ここに複数のキーが見つかった場合は、「IBM MIMEsweeper System」というラベルが付いていないものを削除します。リブートしてください。

大きなファイルのダウンロードで WEBsweeper に問題が発生する

問題の説明

WEBsweeper は、フィルター処理の間にファイルを保管するため、仮想メモリーを使い尽くしてしまった可能性があります。

推奨処置

WEBsweeper サーバーの物理メモリーの量を増やします。

共通問題の解決 - SurfinGate

Microsoft Internet Explorer が開くと SurfinConsole が応答を停止する

問題の説明

Internet Explorer が開くと、SurfinConsole アプリケーションが奇妙な振る舞いをするか、または応答を停止します。これらの 2 つのアプリケーションは対立し、同時には実行できません。

推奨処置

Internet Explorer と SurfinConsole を同時にロードしないでください。

SurfinGate プラグインのパフォーマンスが低下する

問題の説明

SurfinGate プラグインを使用すると、Web を介したモバイル・コードのダウンロードがきわめて遅くなります。

推奨処置

「Next Proxy」フィールドが、SurfinConsole の「Proxy」セクションの中の SecureWay ファイアウォール HTTP プロキシーに設定されていることを確認してください。

付録B. 特記事項

本書において、日本では発表されていないIBM製品（機械およびプログラム）、プログラミングまたはサービスについて言及または説明する場合があります。しかし、このことは、弊社がこのようなIBM製品、プログラミングまたはサービスを、日本で発表する意図があることを必ずしも示すものではありません。本書で、 IBMライセンス・プログラムまたは他のIBM製品に言及している部分があっても、このことは当該プログラムまたは製品のみが使用可能であることを意味するものではありません。これらのプログラムまたは製品に代えて、IBMの知的所有権を侵害することのない機能的に同等な他社のプログラム、製品またはサービスを使用することができます。ただし、IBMによって明示的に指定されたものを除き、これらのプログラムまたは製品に関連する稼働の評価および検証はお客様の責任で行っていただきます。

IBMおよび他社は、本書で説明する主題に関する特許権（特許出願を含む）商標権、または著作権を所有している場合があります。本書は、これらの特許権、商標権、および著作権について、本書で明示されている場合を除き、実施権、使用権等を許諾することを意味するものではありません。実施権、使用権等の許諾については、下記の宛先に、書面にてご照会ください。

〒106-0032 東京都港区六本木3丁目2-31
AP事業所
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム（本プログラムを含む）との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

Site Counsel, IBM SWG
IBM Corporation
P.O. Box 12195
3039 Cornwallis
Research Triangle Park, NC 27709-2195
USA

本プログラムに関する上記の情報は、適切な条件の下で使用することができますが、有償の場合もあります。

本書は、プロダクション使用を目的としたものではなく、いかなる種類の保証も含まれていません。このため、商用および特定の目的への適合性の保証を含め、すべての保証に対し、本書は関与しません。

本製品には、CERN により開発、販売されるコンピューター・ソフトウェアが含まれます。その使用表示は、ここに含まれる CERN コンピューター・ソフトウェアまたはその一部を含む一切の製品において言及されるものとします。

商標

以下の用語は、IBM Corporation の米国およびその他の国における商標です。

AIX

IBM

Microsoft および Windows NT は、Microsoft Corporation の商標または登録商標です。

**SurfinGate は Finjan Software, Ltd. の商標です。

MIMEsweeper、MAILsweeper、および **WEBsweeper は、Content Technologies, Ltd. の商標です。

2 個のアスタリスク (**) で表示された他の会社名、製品名、サービス名等は、それぞれ各社の商標または登録商標です。

用語集

C

クライアント (client). 別のコンピューター・システムまたはプロセス (通常サーバーと呼ばれる) のサービスを要求するコンピューター・システムまたはプロセス。複数のクライアントが、1 つの共通サーバーに共用アクセスができる。

D

デフォルト (default). 明示して何も指定されなかった場合に想定される、値、属性、またはオプション。

DMZ. 非武装地帯 (Demilitarized Zone)。外部のユーザーが、企業データを持つサーバーに直接アクセスできないようにするためのデバイス。

F

ファイアウォール (Firewall). ある 1 つのネットワークから他のネットワークへの接続の保護および制御を行う機能単位。ファイアウォールは、希望しないかまたは無許可の通信トラフィックが保護されたネットワークに入り込むのを防止し、選択された通信トラフィックだけが保護ネットワークを出ていくようにする。

ファイル転送プロトコル (FTP (File Transfer Protocol)). ネットワーク・コンピューター間のファイルの転送に使用されるアプリケーション・プロトコル。リモート・ホスト・システムのファイルをアクセスできるようにするため、 FTP は、ユーザー ID と、場合によってはパスワードを必要とする。

G

ゲートウェイ (gateway). 2 つのコンピューター・ネットワークを異なるアーキテクチャーで相互接続する機能単位。

I

インターネット (Internet). インターネット用のプロトコルの組を使用する、全世界に広がる相互接続ネットワークの集合で、公衆アクセスが許される。

ICMP. インターネット制御メッセージ・プロトコル (Internet Control Message Protocol)。インターネット・プロトコル (IP) レイヤーの中で、エラー・メッセージと制御メッセージを取り扱うために使用されるプロトコル。問題レポートおよび誤ったデータグラムの宛先が、元のデータグラムの送信元に戻される。

イントラネット (intranet). インターネット標準とアプリケーション (Web ブラウザーなど) を、組織の既存のコンピューター・ネットワーク・インフラストラクチャーと統合する、機密保護された私設網。

IP. インターネット・プロトコル (Internet Protocol)。データをネットワークまたは相互接続ネットワークを介して経路指定する、コネクションレス型プロトコル。 IP は、上位のプロトコル層と物理層の間の中間層として働く。

IP アドレス (IP address). インターネット・プロトコル・アドレス (Internet Protocol address)。ネットワーク内のそれぞれのデバイスまたはワークステーションの実際の場所を指定する、固有の 32 ビット・アドレス。これはまた、インターネット・アドレスとも呼ばれる。

IPSEC. インターネット・プロトコル・セキュリティー (Internet Protocol Security)。ネットワークまたはネットワーク通信のパケット処理層における、開発中のセキュリティーの規格。

L

ループバック・インターフェース (loopback interface). 情報が同じシステム内のエンティティーをアドレス指定している場合に、不必要な通信機能をう回するインターフェース。

N

NAT. ネットワーク・アドレス変換 (Network Address Translation)。ファイアウォールにおいて、セキュア IP アドレスを外部の登録済みアドレスに変換すること。これによって外部ネットワークとの通信が可能になるが、ファイアウォール内部で使用される IP アドレスをマスクする。

P

PICS. インターネット・コンテンツの選択用プラットフォーム (Platform for Internet Content Selection)。PICS 可能なクライアントにより、ユーザーは、どれだけの評価サービスを使用したいかを判別し、それぞれの評価サービスごとに、どの評価が受け入れ可能で、どの評価が受け入れ可能でないかを判別することができる。

ping. インターネット制御メッセージ・プロトコル (ICMP) のエコー要求パケットをホスト、ゲートウェイ、またはルーターに応答を受け取ることを期待して送信するコマンド。

ポート (port). 抽象化された通信装置を識別する番号。 Web サーバーは、デフォルトでは、ポート 80 を使用する。

プロトコル (protocol). 通信が行われる場合に、通信システムの機能単位の操作を制御する規則の集合。プロトコルにより、1 バイトからそれぞれのビットが送信される順序など、低いレベルでのマシン相互間のインターフェースの詳細を決定することができる。また、ファイル転送などの、アプリケーション・プログラム間での高いレベルでの交換も決定することができる。

S

サーバー (server). ネットワークを介して他のコンピューターに共用サービスを提供するコンピューターであり、たとえば、ファイル・サーバー、プリント・サーバー、またはメール・サーバーがある。

サーバー・アドレス (server address). ネットワークを介して他のコンピューターに共用サービスを提供する各コンピューター (たとえば、ファイル・サーバー、プリント・サーバー、またはメール・サーバー) に割り当てられた固有のコード。標準の IP アドレスは、32 ビットのアドレス・フィールドである。サーバー・アドレスは、小数点付き 10 進数の IP アドレスかまたはホスト名にすることができる。

サービス (service). 1 つまたは複数のノードによって提供される機能で、たとえば、HTTP、FTP、Telnet がある。

シェル (shell). ユーザーのワークステーションからコマンド・ラインを受け入れて、処理するソフトウェア。 Korn シェルは、使用可能ないくつかの UNIX シェルの 1 つである。

SMTP. シンプル・メール転送プロトコル (Simple Mail Transfer Protocol)。インターネット用のプロトコルの組において、インターネット環境のユーザー間でメールを転送するためのアプリケーション・プロトコルの 1 つ。 SMTP は、メール交換順序およびメッセージ・フォーマットを指定する。このプロトコルは、下層のプロトコルが伝送制御プロトコル (TCP) であることを想定している。

T

TCP. 伝送制御プロトコル (Transmission Control Protocol)。インターネットで使用される通信プロトコル。 TCP は、信頼性のあるホスト間の情報交換を提供する。このプロトコルは、下層のプロトコルとして IP を使用する。

TCP/IP. 伝送制御プロトコル / インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)。それぞれのネットワークに使用されている通信テクノロジーに関係なく、ネットワーク間での通信を可能にするよう設計されたプロトコルの組。

Telnet. 端末エミュレーション・プロトコルであり、リモート接続サービスのための TCP/IP アプリケーション・プロトコルの 1 つ。 Telnet により、サイトのユーザーは、そのユーザーのワークステーションがあたかも直接そのリモート・ホストに接続されているかのようにアクセスできる。

タイムアウト (timeout). 操作のために割り当てられていた時間間隔が経過したこと。

U

UDP. ユーザー・データグラム・プロトコル (User Datagram Protocol)。インターネット用のプロトコルの組において、信頼性のない、コネクションレス型データグラム・サービスを提供するプロトコル。これにより、あるマシンまたはプロセス上のアプリケーション・プログラムは、別のマシンまたはプロセス上のアプリケーション・プログラムにデータグラムを送信することができる。 UDP は、データグラムを送達するために、インターネット・プロトコル (IP) を使用する。

V

VPN. 仮想私設網 (Virtual Private Network)。 2 つ以上のネットワークに接続される、1 つまたはそれ以上のセキュア IP トンネル経路からなるネットワーク。

W

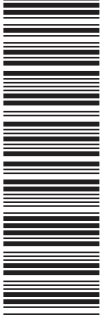
Web. プログラムとファイルが含まれ、それらの多くは HTTP サーバー上の他の文書へのリンクを含むハイパーテキスト文書が含まれている、HTTP サーバーのネットワーク。ワールド・ワイド・ウェブ (WWW) とも呼ぶ。

WTE. Web Traffic Express (WTE)。高度に効率化されたキャッシュ方式を使用して、エンド・ユーザーの応答時間を高速化するのに役立てる、キャッシング・プロキシー・サーバーの 1 つ。柔軟性のある PICS フィルター処理は、 1 つの中央設置場所にある Web ベースの情報にアクセスするのを、ネットワーク管理者が制御するのに役立つ。

ウィザード (wizard). 特定のタスクについてユーザーをガイドするために、ステップバイステップの指示を使用する、アプリケーション内のダイアログ。

部品番号: CT6RZJA

Printed in Japan



CT6RZJA

GC88-8558-00

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12